CyberSecurity
(Emerging Threats, Managing Controls and Best Practices)
Per NCUA

February 10, 2015

E. Andrew Keeney, Esq.
Kaufman & Canoles, P.C.

Slideshow originally prepared by
Jerald L. Garner, MS, CRMA, ISO 27001,
CRISC, CISA, CISSP
National Field Supervisor
National Credit Union Administration
Office of National Examinations and Supervision

Presented today by E. Andrew Keeney, Esq., with permission.

E. Andrew Keeney, Esq.

Kaufman & Canoles, P.C.

150 West Main Street, Suite 2100

Norfolk, VA 23510

(757) 624-3153

eakeeney@kaufcan.com

http://www.kaufmanandcanoles.com/movies/credit-unions.html

- This presentation is for information sharing purposes only. All contents of this presentation are based on my independent research efforts and years of experience. Mention of trade names or commercial products does not constitute endorsement or recommendation of use by NCUA. The existence of hyperlinks does not constitute endorsement by NCUA or of these Web sites or documents or of the information contained therein. Interested parties should do their own research, and the list of references may provide a starting point. Additionally, participants of this presentation assume the risk of use or reliance on such information.

*Disclaimer

Overview

- CyberSecurity
  - ✓ What is it?
  - ✓ What about Information Security?
- Threat Sources
  - ✓ Nation State
  - ✓ Organized Crime (underground)
  - ✓ Hackers
  - ✓ Consumers/EndUsers/Employees
- Recent Events
  - ✓ Threat Environment
    - ❖ Disturbed Denial of Service Attacks (DDoS)
    - ❖ Data Breaches
    - ❖ Open Systems
- Contributing Factors
  - ✓ Consumerization of Information Technology (IT)
- Threat Mitigation
  - ✓ Awareness
  - ✓ Training
  - ✓ Guidance
  - ✓ Policies
- ✓ Best Practices
  - ✓ SANS's
  - ✓ NIST Framework
  - ✓ 2015 Exam Focus
- Questions and Answers

Understanding

CYBERSECURITY

CyberSecurity

- Cybersecurity
  - The process for managing cyber threats and vulnerabilities and for protecting information and information systems by identifying, defending against, responding to, and recovering from attacks.
- Information Security
  - Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. *(Source: FFIEC IT Handbooks – Information Security)*

Cyberattacks

- Cyberattack
  - A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

http://www.techopedia.com

CyberSecurity continued

- Presidential Executive Order
  - 13636
  - February 2013
  - Improving Critical Infrastructure CyberSecurity
- Cybersecurity Framework
  - A set of standards, methodologies, policies and procedures that align policy, business, and technological approaches to manage cyber risks

Threat

ACTORS (SOURCES)

Threats

- Nation State Sponsored
  - South Korea (2013)
    - Banks, Media Outlets
    - Systems Compromised – Patch Management
  - Why?
    - Cyber-attacks
      - Project national power @ low-cost, and
      - High-payoff way to defend national sovereignty
  - Power Grid (US)

The Underground

- Internet source for cybercriminals
  - Buy/sell different products and services
  - 2014 security predictions
    - Leverage Targeted Attacks (TrendMicro)
      - Spear Phishing
      - Remote Access Trojans

Most Requested - Underground

- **Attack Tools**
  - ✓ Programming services and software sales
  - ✓ Hacking services
  - ✓ Dedicated server sales and bulletproof-hosting services
  - ✓ Spam and flooding services, including call and SMS flooding services
    - – *Download sales*
    - – *DDoS services*
    - – *Traffic sales*
    - – *File encryption services*
    - – *Trojan sales*
    - – *Exploit writing services and sales*

Organized Crime

- Organized Crime
  - Low Cost
  - Utilize proofing effective attack tools
  - Effective Attacks
  - Large Payoffs
    - Social engineering attack tricks companies into large wire transfers
      - (May 2014) TrustedSec study
- Consumers (Technology Users, Employees)
  - Utilize advance technology
  - Negligence and user errors
    - Insider Theft soared 80% over 2012 stats
      - Identity Theft Resource Center Study (ITRC) 2014

Media Attention

RECENT EVENTS

Recent Events

- Distributed Denial of Services (DDoS) Attacks
  - Financial and government entities have become the target
  - Increased attack efforts
    - Difficult to defend (3rd party or Internet Service Provider (ISP) involvement)
- Data Breaches
  - 1st Qtr 2014 – 200,000 million records breached (SafeNet)
    - Approximately 93,000 records per hour,
    - 233 percent increase over the same quarter in 2013
  - State Laws – Data Breach notification laws

Recent Events continued

- Incident Sources and Costs
  - Attacks
    - Malicious insider
      - Cost the most ($213,542) (rarest)
    - DDoS attacks
      - Cost ($166,545)
  - Energy and utility organizations priciest attacks ($13.18 million)
  - Financial services ($12.97 million)
- Per-capita
  - Small organizations are higher than large ones ($1,601 versus $437)

Ponemon Institute

Recent Events Continued

- Merchants
  - Target – 30 million card credentials (vendor management)
  - Michaels – Kmart (Oct 2014)
- Banks
  - JPMorgan Chase
    - 76 million, and 7 million businesses
  - Other Financial Institutions (FIs)
- Fast Food
  - DQ – Jimmy Johns
    - POS Malware - BackOff

Recent Events Continued

- Technology Management Issues
  - Open Systems
    - Heartbleed (OpenSSL) - Patch management issue
    - Shellshock Bash
    - NACH - ACH file
  - Microsoft Windows XP (Dropped support April 14, 2014)
    - ATM's (Status)
    - Desktops (Status) - Lifecycle issue

Methods/Process

- Attacking the weakest link
  - Humans
- Unpatched systems
  - Attackers know which systems
- Easy access to code builders and other tools make carrying out attacks easier
- Cybercriminal precisely target individuals with access to information they want

Contributing

FACTORS

Contributing Factors

- Consumerization of Information Technology (IT)

✓ Mobile
- ❖Bring Your Own Device (BYOD)

✓ Social Media
- ❖Messaging

Meship.com

Factors Continued

- Mobile Payments
  - Many Options
    - ISIS - Softcard
    - PayPal – 44%
    - Starbucks
    - Apple Pay
    - Paydiant
- Digital Currency
  - Exchanges
  - Mining

Factors Continued

- Financial Entities Out-Sourcing
  - Cloud
  - Payment Solutions
- Systems Complexity
  - Network Infrastructure
  - Virtualized environment
- Majority of financial services
  - Internet accessible
  - Mobile device capable
  - Requires data encryption in transit and storage
  - Demands continuity of operations procedures

Threat

MITIGATION

Understand the Threats

- Awareness of the Cyber Environment
  - Threat Intelligence
    - Alert Services
      - **SANS - S**ysAdmin, **A**udit, **N**etworking, and **S**ecurity SANS
        - » NewsBites – Executive Summary
        - » @RISK: The Consensus Security Alert - advanced
        - » Ouch! - basic
          - » http://www.sans.org/newsletters/
      - **CERT** – US-**C**omputer **E**mergency **R**esponse **T**eam
        - » Alerts - advanced
        - » Bulletins - advanced
        - » Tips – basic
          - » http://www.us-cert.gov/ncas
    - **NCUA -** http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx

Shifts

- Layered Approaches to Security
  - Confidential, Integrity, and Availability (CIA)
    - Administrative controls
    - Delivery methods (User interface)
    - Data communications
    - Active monitoring
    - Encryption

Training and Guidance

- Training
  - SANS Institute – http://www.SANS.org
  - Multi-State Information Sharing & Analysis Center
    - https://msisac.cisecurity.org/resources/videos/free-training.cfm
  - NCUA/OSCUI
- Guidance
  - NCUA Rules & Regs:
    - 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance, and
    - 12 CFR Part 749: Records Preservation Program
  - FFIEC – Information Technology Manuals

Policy

- Part 748
  - Information Security Program
    - Security Awareness Training Program
    - Incident Response Policy
    - Patch Management Policy
- Part 749
  - Business Continuity Plan/Policy
    - Document Destruction Procedures
    - Pandemic Procedures
    - Response Plan/Policy
    - Disaster Recovery Plan/Policy

Best

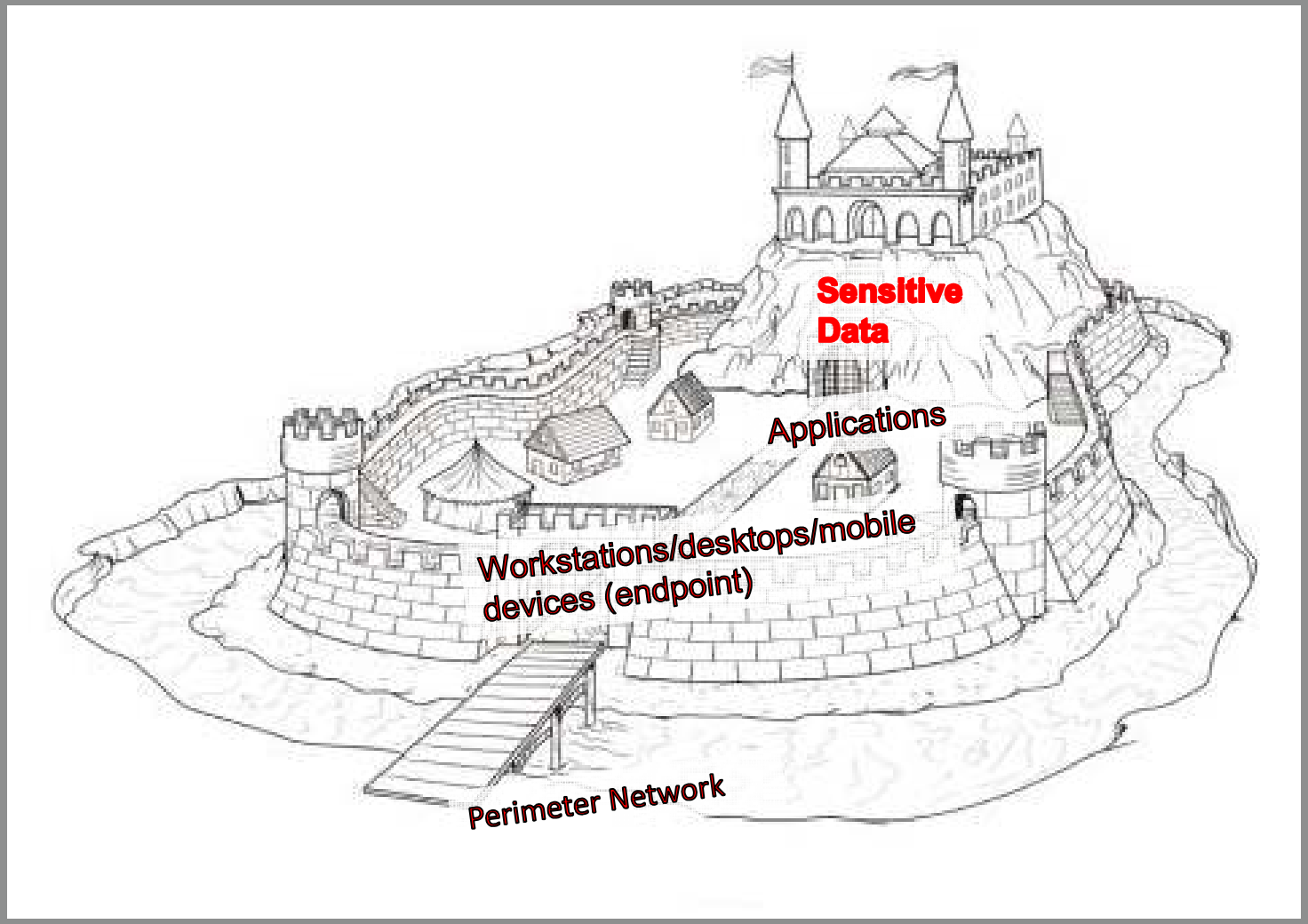
PRACTICES

Best Practices

- Basic's of Information Security
  - Confidential, Integrity, and Availability (CIA)
- Layered Security
  - arises from the desire to cover for the failings of each component by combining components into a single, comprehensive strategy, the whole of which is greater than the sum of its parts, focused on technology implementation with an artificial goal of securing the entire system against threats

http://www.techrepublic.com/

The Layers


Sensitive
Data
Applications
Workstations/desktops/mobile
devices (endpoint)
Perimeter Network

Perimeter Network - 1st Layer of Security

Firewalls (FW), routers (ACL's), and segmented systems

Intrusion Detection / Prevention Systems (IDS/IPS)

Active Monitoring

Workstations/desktops/mobile devices (endpoint) - 2nd Layer of Security

Admin Lockdown

Anti-virus, FW, updates, host IDS, etc

Application - 3rd Layer (service controls) of Security

Authentication Methodology

IP Address Lockdown & Dual Controls, etc

Secure Transactions/privacy data access

Best Practices

- Controls
  - Policies
    - Employee Acceptable Use Policy
    - Social Media Policy
    - Vendor Management Policy
  - Networking Environment
    - Utilize Firewalls
    - Intrusion Detection and Prevention (ID/IP) Systems
  - Desktop and Server
    - Malware Protection (Anti-Virus)
    - Administrative Permissions
    - Patch Management Program

Breach Ready Credit Union

- Maintain
  - Current network diagram that shows data flows
- Logs – critical ones
  - Security Logs
    - Server and workstation operating system logs
    - Application logs (e.g., web server, database server)
    - Security tool logs (e.g., anti-virus, change detection, intrusion detection/prevention system, end-user apps)
- Hostname-IP addresses
  - Dynamic Host Configuration Protocol (DHCP) rotates the mapping of IP addresses to internal systems

Breach Ready continued

- Know how to find files in your environment
  - If malicious files are spotted on the network
  - Be able to locate where that file exists
- Incident Response Plans
  - Incident Response Policies and procedures are controls – test them!
- Public notification – know the answers
  - What and how it happen?
  - Prevention and protection steps

Cyber Security

- National Institute of Science and Technology (NIST) - The ability to protect or defend the use of cyberspace from cyber attacks.
  - The National Institute of Science and Technology (NIST) developed a Cybersecurity Framework for critical industry entities
  - Basic Cybersecurity/information security functions (CORE)
    - Identify (Asset inventory/risk assessments; systems, software, hardware, personnel, information, etc)

2015 Examination Focus

- IS&T
  - eBanking
  - Business Continuity Planning
  - Vendor Management
  - Cyber Security
- Payments
  - Ach
  - IP/RDC
  - Wires

Sources

http://www.cert.org/insider-threat/

http://www.us-cert.gov/ncas

http://www.sans.org/newsletters/

http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx

http://www.ready.gov

http://www.prolexic.com/knowledge-center/

http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

http://www.privacyrights.org/data-breach

E. Andrew Keeney, Esq.

Kaufman & Canoles, P.C.

150 West Main Street, Suite 2100

Norfolk, VA 23510

(757) 624-3153

eakeeney@kaufcan.com

http://www.kaufmanandcanoles.com/movies/credit-unions.html

CyberSecurity (Emerging Threats, Managing Controls and Best Practices)

February 10, 2015

E. Andrew Keeney, Esq.
Kaufman & Canoles, P.C.